Physical Security checklist #1 & #2 (section 3.11.2)

February 1, 2011

The left column indicates whether the standard is listed in the Information Security Plan as a Must or Should. A justification must be written for any standard not followed in the department procedures. The justification must be approved by the IT Manager for items listed as a Should and also reviewed with the IT Security Office if the item was listed as a Must. The IT manager must review, sign and date, all exceptions every six months to indicate that the exception is still necessary.

M/S	Item	Y/N
S	1. Server room	
S	❖ Minimize number of server rooms needed	
S	❖ Utilize card access	
S	❖ Visitors/contractors escorted at all times	
S	❖ Room not duel purposed for functions with uncontrolled access (office supplies, etc.)	
	2. Doors	
S	❖ Locked and accessible by authorized key or manual key backup for card access	
S	❖ Constructed with one-hour fire rating	
S	❖ Resistant to being forced open	
S	❖ Fail-safe during power interruption (requiring key access and any exit)	
S	❖ Self-closing with no hold-open feature	
S	❖ With card access, alarm should trigger if door forced open or held open for extended period of time	
	3. Windows	
S	❖ Server room should not have windows	
S	❖ If windows, too small for physical entry	
S	❖ If windows, blinds or reflective file used to limit visibility	
S	❖ If windows, additional bars to prevent theft of equipment or information	
S	❖ Self-closing with no hold-open feature	
	4. Fire Safety	
S	❖ IT manager ensure controls exist to manage sources/factors that can lead to fires (faulty electric devices/wiring, unattended heating, combustible materials)	
S	❖ IT manager ensure fire extinguishing systems are located in the server room (portable or large scale depending on location)	
	5. Electrical Systems	
S	❖ Use configurable Uninterruptible Power Supplies (UPS) for both power supply conditioning and redundancy	
S	❖ Monitor the amount of power being drawn if multiple machines are plugged into a single power strip	
S	❖ Use antistatic carpeting to protect against static electricity	
S	❖ Use line conditioners or surge protectors to protect desktop systems	
S	❖ Ensure there is a readily available emergency power off switch to shut down the power quickly if required, preferably a single switch for all systems, near an exit, and covered to protect against accidental activation	
S	❖ Ensure automatic generator backup	
S	❖ Request review of power use and electrical system controls by Physical Plant	

	when significant equipment changes	
	6. HVAC	
S	❖ Critical servers should never be placed directly below water pipelines or air conditioner condensers, in case of leaks	
S	❖ IT management should ensure that IT support staff know the location of all relevant shutoff valves and understand the procedure that should be followed in the event off a water line failure	
S	❖ IT managers should request a review of plumbing and cooling system use and controls by Physical Plant when there are significant changes in the building architecture	
	7. Temperature & humidity ranges	
S	❖ IT managers should ensure that temperature and humidity ranges are within acceptable levels and monitored	
S	❖ IT management should ensure that IT support staff know the location of all relevant shutoff valves and understand the procedure that should be followed in the event off a water line failure	
	❖ An automated alert system should be configured to notify the IT manager when temperature and humidity ranges are outside acceptable levels for all critical systems	